

# Exhibit 1



or suspected terrorists in the TSDB. TSA uses the results of this process to require such individuals to undergo enhanced security screening prior to boarding an aircraft or to deny boarding. TSA also uses the TSDB as a part of its process in conducting security threat assessments on individuals who seek access to sensitive transportation systems and information, including pilots, aviation workers, and other individuals who have inside access to the aviation system.

4. The TSDB is key to TSA's ability to counter ongoing terrorist threats. While aviation security operations have advanced significantly since TSA's creation, the United States still faces determined adversaries. Terrorists remain intent on attacking civil aviation, and the threat environment remains complex, diverse, and persistent. The TSDB remains an essential and effective component of TSA's countermeasures in substantial part because its contents are not disclosed to individuals required to undergo enhanced security screening.<sup>1</sup>

5. As set forth below, I first describe TSA's mandate and highlight security measures used by TSA to secure aviation. Next, I describe the current threat to aviation, including recent attempts to commit terrorist attacks. I then describe the security measures TSA uses to counteract the threat posed by terrorists, and the effect that disclosing status in the TSDB to those required to undergo enhanced screening would have on those security measures. Finally, I describe TSA's limited disclosures of TSDB information and how TSA ensures the confidentiality of that information.

---

<sup>1</sup> This declaration is limited to public information and thus necessarily omits certain supporting detail regarding the threats and challenges that TSA must address and counteract.

### TSA's Mandate and Security Measures

6. As a result of the terrorist attacks of September 11, 2001, Congress passed the Aviation and Transportation Security Act of 2001 (ATSA),<sup>2</sup> which created TSA. ATSA charged TSA with responsibility “for security in all modes of transportation” and created a federal workforce to screen passengers and cargo at commercial airports.<sup>3</sup> ATSA also granted TSA broad authority to “assess threats to transportation,”<sup>4</sup> to “develop policies, strategies, and plans for dealing with threats to transportation security,”<sup>5</sup> to “enforce security-related regulations and requirements,”<sup>6</sup> and to “oversee the implementation, and ensure the adequacy, of security measures at airports.”<sup>7</sup> ATSA also specifically directed TSA to take appropriate action with respect to individuals who may be a threat to civil aviation or national security.<sup>8</sup>

7. Congress further directed TSA to assume from aircraft operators the function of conducting pre-flight comparisons of airline passenger information to Federal government watchlists for domestic flights and international flights to, from, and overflying the United States.<sup>9</sup>

8. TSA executes its mandate in substantial part through the Secure Flight program, its advanced passenger prescreening program which compares passenger

---

<sup>2</sup> Pub. L. No. 107-71, 115 Stat. 597 (2001).

<sup>3</sup> ATSA § 101, 49 U.S.C. § 114(d); ATSA § 111, amending 49 U.S.C. § 44935.

<sup>4</sup> 49 U.S.C. § 114(f)(2).

<sup>5</sup> 49 U.S.C. § 114(f)(3).

<sup>6</sup> 49 U.S.C. § 114(f)(7).

<sup>7</sup> 49 U.S.C. § 114(f)(11).

<sup>8</sup> See ATSA § 101, 49 U.S.C. §§ 114(f), 114(h)(3).

<sup>9</sup> Pub. L. No. 108-458, 118 Stat. 3638, Dec. 17, 2004; 49 U.S.C. § 44903(j)(2) (The Intelligence Reform and Terrorism Prevention Act of 2004).

information to various Government watchlists.<sup>10</sup> Secure Flight may designate an individual for enhanced, standard, or expedited screening at airport security checkpoints or may result in denial of boarding.

9. Aviation passengers must undergo security screening prior to entering the sterile area of an airport and boarding an aircraft.<sup>11</sup> On an average day, TSA screens over two million passengers and six million items of carry-on and checked luggage.<sup>12</sup> Of these passengers, Secure Flight designates a very small percentage for enhanced screening.

10. Secure Flight may designate aviation passengers for enhanced screening for a variety of reasons, including random selection, matching to one of TSA's risk-based rules,<sup>13</sup> TSDB status, or for other reasons.<sup>14</sup> For purposes of Secure Flight matching to the TSDB, TSA may designate passengers for enhanced screening who meet the

---

<sup>10</sup> Secure Flight matching is limited to covered aircraft operators, which are generally airlines offering scheduled and public charter flights from commercial airports. Secure Flight does not conduct watchlist matching for non-covered aircraft operators. TSA instead provides exports of the No Fly and Selectee subsets of the TSDB to regulated U.S. aircraft operators operating charters and other flights under a TSA-authorized security program on aircraft that are not covered by Secure Flight and those entities are responsible for completing the watchlist matching function for their aviation passengers. As further described below, there are strict controls over access to and the use of those subsets of the TSDB.

<sup>11</sup> The sterile area refers to portions of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, an aircraft operator, or a foreign air carrier.

<sup>12</sup> TSA agents will discover an average of 11.6 firearms, ten of which are loaded, in carry-on luggage every day. <https://www.tsa.gov/blog/2019/02/07/tsa-year-review-record-setting-2018>.

<sup>13</sup> My declaration of August 15, 2018 further describes TSA's risk-based rules. TSA uses two sets of risk-based rules to designate passengers for enhanced security screening, referred to as Silent Partner and Quiet Skies. Silent Partner rules apply to passengers on international flights and Quiet Skies rules are a subset of Silent Partner rules that apply to domestic screening operations. As directed by Congress, the DHS Traveler Redress Inquiry Program (DHS TRIP) is available to individuals who experience travel difficulties related to matching one of TSA's risk-based rules. FAA Reauthorization Act of 2018, § 1949(a). In addition, TSA has robust review procedures for its risk-based rules within TSA and with the DHS Privacy Office, Office for Civil Rights and Civil Liberties and Office of the General Counsel.

<sup>14</sup> TSA does not identify individuals for enhanced screening as a result of any prior but not current listing in the TSDB. TSA's screening operations, including reasons for designating individuals for enhanced screening, are subject to oversight by the DHS and TSA Civil Rights and Civil Liberties Offices, Privacy Offices, and Legal Counsel Offices to ensure compliance with the U.S. Constitution, applicable laws and regulations, and DHS and TSA policy.



reasonable suspicion standard for TSDB inclusion and for whom the TSDB record contains a full name and a full date of birth.<sup>15</sup> In contrast, individuals who meet additional heightened substantive derogatory criteria for inclusion on the No Fly List, a separate subset of the TSDB, generally are not allowed access to sterile areas of airports and are denied boarding. The majority of passengers designated for enhanced security screening are so designated for reasons other than TSDB status.

11. Individuals included in the TSDB may be designated for enhanced screening on multiple consecutive flights. Individuals who are not in the TSDB may also be designated for enhanced screening on multiple consecutive flights, diminishing the ability of any individual to infer TSDB status from repeated designation for enhanced screening.

12. TSA applies the same checkpoint screening procedures to individuals Secure Flight designates for enhanced screening, regardless of whether the individual is designated due to TSDB status, randomly, or for other reasons. The passenger's boarding pass does not include the reason for the enhanced screening designation. In addition, passengers designated by Secure Flight for expedited or standard screening are not guaranteed to receive that type of screening and may be required to undergo additional or enhanced screening as a result of unpredictable and random screening measures at the

---

<sup>15</sup> Individuals who meet this minimum requirement are included in the Expanded Selectee List. The Selectee List, a separate subset of the TSDB, requires additional heightened substantive derogatory criteria to be met before the individual is added to the Selectee List. While TSA applies the same checkpoint procedures to individuals on the Expanded Selectee List as individuals on the Selectee List, TSA values having separate Selectee and Expanded Selectee Lists. More specific details related to why TSA values having both subset lists constitutes Sensitive Security Information.

checkpoint, to resolve an alarm generated by a walk-through metal detector or Advanced Imaging Technology (AIT),<sup>16</sup> or for other reasons.

13. TSA recommends that all travelers arrive two to three hours in advance of the scheduled flight time. Although passengers may be delayed as a result of TSA's security measures, the purpose and effect of these measures is to ensure aviation security and the freedom of movement for people and commerce.

14. TSA's security measures extend beyond TSA security checkpoints. TSA uses unpredictable security measures throughout the airport to accomplish its transportation security mission. All passengers may be required to undergo additional screening at boarding gates, which is conducted after clearing initial checkpoint screening.

15. The Federal Air Marshal Service (FAMS) also represents a necessary security measure to mitigate threats.<sup>17</sup> Federal Air Marshals are deployed on commercial aircraft using risk-based analysis, and as such, FAMS missions are responsive to current intelligence, threats, and vulnerabilities. FAMS' mission coverage goals are adjusted continually in response to emerging and evolving threats and incorporate randomness and unpredictability as a further mitigation measure. Federal Air Marshals serve as a deterrent to those who intend to do harm, and they have multiple priorities during flight, including protecting the flight deck and passengers in the cabin from terrorist attacks. In

---

<sup>16</sup> The AIT is designed to identify both metallic and non-metallic potential threat items that may be concealed on an individual.

<sup>17</sup> Congress directed TSA to deploy Federal Air Marshals to passenger flights that present high security risks and to utilize a risk-based strategy when making Federal Air Marshal resource allocation decisions for domestic and international flights. 49 U.S.C. § 44917. Congress requires TSA to consider its risk-based rules when creating Federal Air Marshal mission schedules. FAA Reauthorization Act of 2018, §1949(d)(1).

carrying out their responsibilities, Federal Air Marshals observe what any other passenger or the flight crew could observe.

16. Large populations of individuals have insider access to secure areas of airports and other transportation venues. As demonstrated by news reporting related to recent terrorist attacks, this access could allow insiders to provide necessary materials or weapons to individuals to carry out a terrorist attack. To counter this threat, TSA implements several security measures and controls, including requiring a security threat assessment for such individuals. TSA uses governmental databases and available information, including the TSDB, as part of its security threat assessment process.

#### The Current Threat

17. Aviation remains a principal target for terrorists who seek to instill fear, disrupt the economy, and undermine the American way of life. Terrorists are constantly working to find new methods for disguising explosives, recruiting insiders, and hijacking aircraft.

18. The United States continues to face one of the most challenging threat environments since 9/11, as foreign terrorist organizations exploit social media and secure communication applications to inspire, enable, or direct individuals already here in the United States to commit terrorist acts.

19. Terrorist groups have proven adaptive in the face of new security measures, as demonstrated by their development of non-metallic explosive devices designed to evade metal detectors and other aviation security measures. These devices remain some of the most serious threats to aviation. The threat is compounded by the



fact that terrorist groups have published instruction manuals online and invited their aspirants to use the information.

20. One such example is the 13th edition of Inspire, Al-Qaeda in the Arabian Peninsula's (AQAP) English language magazine. Published in December 2014, Inspire 13 focuses on lone actor attacks and presents detailed instructions for constructing a bomb, proceeding with it through airport security, and detonating it onboard while over U.S. soil.

21. Since 2015 terrorist groups' have broadened the scope and location of aviation attacks, as shown by the attacks on commercial aircraft in Egypt and Somalia, in 2015 and 2016, respectively, and the 2017 terrorist plot in Australia. These plots are sobering reminders that the threat to aviation is as real as ever.

22. In October 2015, Metrojet Flight 9268 was scheduled to fly from Sharm el-Sheikh International Airport, Sinai Peninsula, Egypt to St. Petersburg, Russia, but suffered a catastrophic explosive event after departing, killing all 224 passengers. Islamic State of Iraq and ash-Sham (ISIS) claimed responsibility. Following an investigation, several countries, including the United States, concluded that the plane was brought down by an explosive device. A matter of significant concern about the bombing was the possibility of an airport worker facilitating the smuggling of the bomb onto the plane.

23. In the wake of the Metrojet attack, ISIS published a new edition of their English language magazine Dabiq, which celebrated the downing of the aircraft and displayed a photo of the improvised explosive device (IED) purportedly used to bring down the aircraft. The photo revealed a soda can filled with a substance—possibly an

explosive—a commercial detonator, and a probable firing circuit that could include a timer and power source.

24. In February 2016, a bomb detonated onboard Daallo Airlines Flight D3-159 from Mogadishu, killing only the bomber. Al-Qaeda linked terrorist group al-Shabaab claimed responsibility. Per media reports, Somalia's government spokesperson noted that security video footage taken at Mogadishu airport showed the suspected suicide bomber being handed what appears to be a laptop computer by an individual dressed as an airport worker after passing through the security checkpoint. Media reports called this a clear example of terrorists mastering the technique of getting simple bombs on planes via corrupt airport personnel.

25. In the summer of 2017, a plot was uncovered highlighting threat actors' efforts to detonate a bomb on a flight from Sydney, Australia with explosive material hidden in a meat grinder. Australian Federal Police called it one of the most sophisticated plots that had ever been attempted on Australian soil. An alleged senior ISIS commander likely sent parts, including weapons-grade explosives, from Turkey to develop a bomb intended to bring down an airliner leaving Australia. The plot was reportedly only aborted after the luggage with the device was deemed overweight.

26. In 2017, the United States became increasingly concerned about the terrorist threat to civil aviation, as terrorist groups such as al-Qaeda affiliates AQAP to al-Shabaab, and from al-Qaeda to ISIS expressed interest in concealing IEDs in modified electronic devices, including laptops, printers, and cameras. The success of ISIS in downing one commercial airliner (Metrojet) underscores their capability and intent to pose a persistent threat to aviation.

27. This background indicates that terrorist groups continue to see this Nation's civil aviation system as a highly valuable target. Terrorist groups are expected to continue to use insiders to execute attacks and also to apply their ingenuity to devise new ways to bypass or defeat aviation security measures. Terrorist groups will likely continue to share information on weapons, tactics, and targets in online publications and social media in order to incite lone actor attacks.

#### Security Measures to Mitigate the Threat

28. Applying enhanced screening and other appropriate security measures to known or suspected terrorists in the TSDB is essential to prevent attacks against civil aviation and the Nation. These are individuals that U.S. law enforcement and intelligence agencies have reasonable suspicion to believe are engaged, have been engaged, or intend to engage, in conduct constituting, in preparation for, in aid or in furtherance of, or related to, terrorism and/or terrorist activities. For example, individuals may be included in the TSDB due to membership in terrorist organizations that pose a grave threat.

29. Below I describe TSA security measures and TSA's use of the TSDB. I further describe how the effectiveness of TSA security measures would be diminished by the disclosure of status in the TSDB to individuals who are required to undergo enhanced security screening.

#### *Pre-Screening and Watchlist Matching*

30. Pursuant to section 4012(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), TSA implemented the Secure Flight program. Under

this program, covered aircraft operators<sup>18</sup> must transmit to TSA certain passenger information for flights into, out of, within, and over the U.S., and on point-to-point international flights operated by U.S. airlines, approximately 72 hours prior to scheduled flight departure times.<sup>19</sup>

31. Secure Flight uses the passenger information it receives from aircraft operators to determine if any passengers are on a Government watchlist such as the TSDB.<sup>20</sup> After Secure Flight completes the comparison of passenger information, TSA provides instructions to aircraft operators to identify the individual for standard, enhanced, or expedited screening at a security checkpoint, or to deny the individual transport or authorization to enter a U.S. airport's sterile area.<sup>21</sup> TSA may designate passengers for enhanced screening for a variety of reasons other than status on the TSDB, as described above.

32. In the case of an individual requiring enhanced security screening, the aircraft operator applies a "SSSS" marking on the boarding pass to signify that enhanced screening is required. The notation applies to all passengers designated for enhanced screening, including individuals designated by random selection or for other reasons unrelated to the TSDB. There is no special notation on passengers' boarding passes to

---

<sup>18</sup> These aircraft operators generally are the passenger airlines that offer scheduled and public charter flights from commercial airports.

<sup>19</sup> For reservations created within 72 hours of flight departure, including reservations booked by walking up to an airport ticket counter, covered aircraft operators must submit Secure Flight passenger information as soon as it becomes available. Aircraft operators may not issue a boarding pass to a passenger until TSA responds.

<sup>20</sup> TSA obtains its export of the TSDB via the Department of Homeland Security (DHS) Watchlist Service (WLS). WLS maintains a synchronized copy of the TSDB and disseminates exports of TSDB records to authorized DHS Components, including TSA.

<sup>21</sup> Some passengers designated for enhanced screening may be required to check-in at the airport ticket counter instead of checking in online or using an airport kiosk. An airline representative may ask the individual for identification and may place a call to TSA for identity resolution. During these calls, TSA does not disclose whether or not the individual is in the TSDB and will only provide the representative with instructions to identify the individual for standard, enhanced, or expedited screening at a security checkpoint, or to deny boarding. The average time for such calls is 12.5 minutes.

signify inclusion in the TSDB or any of its subset lists. TSA then distributes the information within the agency to drive risk-based operational responses and allocation of airport screening resources.

33. Secure Flight pre-screening is one of the Nation's front-lines of defense against terrorism targeting aviation. The Secure Flight program is an essential tool that enables TSA to effectively rely on law enforcement and intelligence information to require known and suspected terrorists in the TSDB and other individuals to undergo enhanced security screening prior to accessing the sterile area of airports and boarding an aircraft.

#### *Checkpoint Screening*

34. All passengers must first undergo screening at an airport security checkpoint before entering the sterile area and boarding an aircraft. Designating passengers for enhanced, standard, or expedited screening allows TSA to carry out this mandate and to focus its limited resources on passengers who present a higher risk or unknown risk while ensuring the freedom of movement for people and commerce. In creating TSA, Congress required TSA to implement "trusted passenger programs and to use available technologies to expedite the security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening."<sup>22</sup>

---

<sup>22</sup> ATSA § 109(a)(3), 49 U.S.C. § 114 NOTE.



35. The value of enhanced security screening is substantial. Assessments show that TSA screeners are more likely to detect prohibited items during checkpoint screening for passengers who are designated for enhanced security screening.<sup>23</sup>

36. TSA continues to adapt its checkpoint security screening measures to better address the threat to our Nation's aviation security. TSA's security measures are informed by intelligence and ongoing threats to aviation. For example, TSA revised its airport screening procedures to account for the December 2001 attempt by Richard Reid (who claimed to be with Al-Qaeda) to detonate explosives packed into the shoes he was wearing while on an American Airlines flight from Paris to Miami; the 2004 attack on two domestic Russian passenger planes using explosives that were concealed on the torsos of female passengers; the 2006 plot to board aircraft with liquid explosives that would be used to construct and detonate a bomb on flights from the United Kingdom to the United States and Canada; and the 2009 attempt of Umar Farouk Abdulmutallab to detonate an explosive device concealed in his underwear on a Northwest flight from Amsterdam to Detroit, for which AQAP claimed responsibility. More recently, TSA revised its security requirements at Last Point of Departure airports with flights to the United States to account for the 2010 discovery of packages containing chemically-initiated IEDs found on cargo planes bound from Yemen to the United States; the 2014 terrorist plots to conceal IEDs in consumer electronics; and the more recent plots and attacks discussed above.

37. Checkpoint screening for all passengers includes screening of the person and his or her accessible property. Below I describe the screening procedures utilized by

---

<sup>23</sup> Specific statistics demonstrating this point are classified.

TSA screeners at checkpoints for standard, expedited, and enhanced screening.<sup>24</sup> I also describe the measures TSA takes at international airports that serve as Last Points of Departure to the United States (LPDs).

38. Standard screening typically includes screening of the person through a walk-through metal detector, the AIT, or a pat-down, and screening of the passenger's accessible property through a scanner. Expedited screening typically includes screening of the person through a walk-through metal detector and accessible property through a scanner.<sup>25</sup> Individuals selected for standard or expedited screening may undergo additional screening of their person (e.g. walk-through metal detector, AIT, and/or a pat-down<sup>26</sup>) and their accessible property (e.g., an explosives trace detection search involving a device certified to detect explosive particles and/or additional physical searches of the passenger's accessible property) for a variety of reasons, including random and unpredictable security measures or an alarm during the screening process.

39. Enhanced screening similarly includes screening of the person and his or her accessible property. The key difference is that TSA is using more than one screening mechanism to clear the passenger and his or her accessible property into the sterile area. Enhanced screening typically includes screening of the person through a walk-through

---

<sup>24</sup> Expedited screening applies to passengers TSA has determined in its sole discretion pose a low risk.

<sup>25</sup> Passengers selected for standard screening are generally required to remove their shoes, laptops, liquids, belts and light jackets, among other things. Passengers selected for expedited screening are not required to remove those items.

<sup>26</sup> A pat-down for all passengers, whether designated for standard, enhanced, or expedited screening, may include inspection of the head, neck, arms, torso, legs, and feet. This includes head coverings and sensitive areas such as breasts, groin, and the buttocks. TSA screeners use the back of the hands for pat-downs over sensitive areas of the body. In limited cases, additional screening involving a sensitive area pat-down with the front of the hand may be needed to determine that a threat does not exist. Pat-downs are conducted by a screener of the same gender and all passengers may request a private screening accompanied by a companion of the passenger's choice. A second screener of the same gender will be present during the private screening.

metal detector, the AIT, and a pat-down, and screening of accessible property through a scanner, an explosives trace detection search, and physical search of the interior of the passenger's accessible property, electronics,<sup>27</sup> and footwear. A typical enhanced screening process takes 10 to 15 minutes.<sup>28</sup> In the event of an alarm, appropriate screening personnel, which may include a TSA explosives expert, will complete the passenger's screening. Enhanced screening may be conducted in any screening lane and there is no special lane or area designated for enhanced screening. In addition, all passengers, whether designated for enhanced, standard, or expedited screening, may request a private screening.

40. TSA trains its personnel to treat all passengers with dignity and respect, regardless of the type of screening for which they are designated. TSA screeners perform administrative searches for items prohibited from entering the sterile area of an airport, such as explosives, weapons, and incendiaries. Generally, TSA screeners are not required to question individuals during the administrative search for any purpose other than facilitating and completing the search,<sup>29</sup> and TSA only requires individuals to remain at the checkpoint until the administrative search is completed. An individual's designation for enhanced screening is not a basis for detaining or questioning the individual. TSA screeners do not seize evidence, arrest individuals, execute criminal investigative searches, or carry weapons. If while performing the administrative search a

---

<sup>27</sup> As a screening measure, TSA does sometimes require electronic devices to be powered on, but TSA does not search electronic devices for electronic content that may be contained on the device, and does not extract data from passenger electronic devices.

<sup>28</sup> This timeframe is based on limited information and applies from when screening commences to its completion. This timeframe does not include any time spent waiting to present boarding pass and identification or following the completion of the screening process.

<sup>29</sup> For example, TSA screeners may ask passengers questions related to whether there are painful areas to touch, whether the passenger can stand for a few minutes for a pat-down, and whether the passenger has any items in accessible property that are sharp or dangerous.

TSA screener discovers a suspected illegal item such as controlled substances or child pornography, the local police will be notified. Upon arrival, local law enforcement officers may conduct a search, seize evidence, and/or effectuate an arrest, pursuant to the statutes, rules, and other authorities governing their conduct.

41. If the screener discovers a prohibited but not illegal item that may not enter the sterile area of the airport, such as a baseball bat, the screener is not permitted to seize the item and rather must give the individual the option of leaving the sterile area to dispose of the item, placing it in checked baggage (if the item is permitted to be carried in checked baggage), leaving it with someone not entering the sterile area, taking it back to his or her vehicle, or voluntarily abandoning it.

42. For purposes of international flights, TSA implements security measures at foreign airports that serve as LPDs to further secure the Nation's aviation system. While TSA screeners do not carry out screening at LPDs, TSA works closely with foreign airports and air carriers to maintain aviation security standards abroad. Foreign countries are generally held to the aviation security standards required by the International Civil Aviation Organization (ICAO), which are minimum baseline requirements. TSA directly assesses the security posture of LPDs and evaluates the implementation of the ICAO standards. Congress has also directed TSA to improve international aviation security standards and to develop a validation process for security equipment to ensure consistency between TSA and foreign partners.<sup>30</sup>

43. TSA also utilizes its regulatory authorities over air carriers serving the United States to require implementation of additional security measures at foreign

---

<sup>30</sup> See FAA Reauthorization Act of 2018, §§ 1914, 1956.

locations. As an element of each air carrier's approval to operate commercial aircraft to, from, or over the United States, the airline agrees to meet all security requirements stipulated by TSA. TSA inspects airlines to ensure all U.S. regulations and international security standards are being met at LPDs.

44. Although the United States has instituted robust aviation security measures since 9/11, evaluated intelligence indicates that terrorist groups' efforts to execute an attack against the aviation sector are persistent given that such attacks provide an opportunity to cause mass casualties and inflict significant economic damage, as well as generate heavy media coverage. One vital way of reducing the risk of an explosive entering the sterile area at LPDs and ultimately ending up on a plane bound for the United States is passenger pre-screening through Secure Flight. Every passenger and crew member on every flight bound for or overflying the United States is required to be vetted against the TSDB, which in turn ensures that known or suspected terrorists receive enhanced screening at foreign airports prior to flying as a passenger to the United States.

#### *Post-Checkpoint Security Measures*

45. TSA's security measures extend beyond TSA security checkpoints. TSA uses unpredictable security measures throughout the airport to accomplish its transportation security mission.

46. All passengers may be required to undergo additional screening at their boarding gates, after they have cleared initial checkpoint screening. Gate screening typically involves randomly selecting a subset of passengers for additional screening at the gate and may include identification checks, searching a person and/or his or her accessible property, and explosive trace detection testing.



47. TSA conducts gate screening for many reasons. For example, local TSA leadership at airports may direct gate screening for any flight to mitigate insider threats and the potential of passengers receiving prohibited items in sterile areas.

48. TSA also utilizes Federal Air Marshals (FAMs) to mitigate risks at the airport and in-flight. Decisions to deploy FAMs are based upon many factors. The identity of flying FAMs constitutes SSI. FAMs generally operate covertly and only reveal their identities when deemed necessary to respond to an immediate threat.

*Countering Insider Threat Using Security Threat Assessments*

49. To carry out its statutory responsibilities, TSA has issued regulations that establish eligibility requirements for individuals who seek access to sensitive transportation areas and systems regulated by TSA. *See, e.g.*, 49 C.F.R. parts 1540 and 1572. TSA conducts security threat assessments on a range of individuals with privileged access to the transportation sector, including those with access to Security Identification Display Areas, sterile areas, and Air Operations Areas at U.S. airports.<sup>31</sup> TSA conducts security threat assessments to ensure that applicants who seek such access meet the eligibility standards of the program to which they apply. For example, in determining whether to grant or deny a Transportation Worker Identification Credential or Hazardous

---

<sup>31</sup> The Security Identification Display Area (SIDA) refers to portions of an airport, specified in the airport security program, in which security measures required by regulation must be carried out. This area includes the security area and may include other areas of the airport. As noted above, the sterile area refers to portions of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, an aircraft operator, or a foreign air carrier. The Air Operations Area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas, for use by aircraft regulated under 49 C.F.R. part 1544 or 1546, and any adjacent areas (such as general aviation areas) that are not separated by adequate security systems, measures, or procedures.

Materials Endorsement, TSA determines whether the applicant poses or is suspected of posing a threat to national security, to transportation security, or of terrorism.<sup>32</sup>

50. In conducting security threat assessments, TSA's eligibility determinations draw on information provided from multiple federal databases, including the TSDB. If TSA's database checks reveal a potential concern, TSA will review the available substantive information and other available relevant information regarding the applicant against the eligibility standards of the particular program to which the applicant belongs. An individual's inclusion in one or more government databases is not determinative of TSA's eligibility determination and merely serves as a factor indicating that an individual requires further scrutiny.

51. Individuals who are required to undergo a security threat assessment by TSA are automatically vetted against the TSDB and other federal databases on a daily basis. Recurrent vetting ensures TSA is made aware of individuals with privileged access to transportation systems who may have connections to terrorism so that TSA can determine whether the individual is eligible to retain privileged access to the transportation sector.

*Disclosure of TSDB Status Would Be Detrimental To Transportation Security*

52. TSA's security measures remain effective in combating terrorism because status in the TSDB is not disclosed to those required to undergo enhanced screening. An individual's status on the subsets of the TSDB that TSA uses for passenger pre-board screening constitutes Sensitive Security Information (SSI) pursuant to 49 U.S.C. § 114(r)

---

<sup>32</sup> 49 C.F.R. § 1572.5(a)(1); *see also* 49 C.F.R. § 1570.3 (defining "security threat").

and 49 C.F.R. part 1520, as TSA has determined that its disclosure would be detrimental to transportation security.<sup>33</sup> Section 1520.5(b)(9)(ii) makes clear that “SSI includes information and sources of information used by a passenger or property screening program or system, including an automated screening system. This is intended to cover information used by a computerized passenger screening system, including lists of individuals identified as threats to transportation or national security.”<sup>34</sup> Disclosure of SSI is limited to covered persons who have a need to know to carry out their official duties and unauthorized disclosure of SSI is grounds for a civil penalty and other enforcement or corrective action.

53. As explained in the Final Order on Sensitive Security Information of April 23, 2018, attached hereto as Exhibit A, if the government revealed the status of individuals as being either on or off the subsets of the TSDB that TSA uses for passenger pre-board screening, terrorists and others who seek to circumvent the purpose of those lists would be able to do so, as they would be armed with the knowledge of who would be required to undergo additional screening and who would not. Terrorists could use the information to attempt to evade enhanced security screening and other security measures to gain access to the commercial aviation system to perpetrate an attack.

54. With respect to Secure Flight matching, official confirmation that an individual required to undergo enhanced screening is in the TSDB could result in evasion of matching, as the individual would be armed with the knowledge that enhanced screening and potentially other security measures will ensue based on reservation data

---

<sup>33</sup> In certain limited circumstances, a U.S. citizen or lawful permanent resident who is denied boarding may learn of his or her status on the No Fly List, a subset of the TSDB, after filing an inquiry with DHS TRIP about the denial of boarding. In those limited circumstances, No Fly List status is not SSI.

<sup>34</sup> 69 Fed. Reg. 28066-1 (2004).

submitted to TSA. The individual could attempt to manipulate reservation data or proof of personal identification in an effort to avoid enhanced screening and other security measures. Through such attempts to manipulate reservation data or proof of identification, a known or suspected terrorist could gain insight into matching thresholds used by Secure Flight to identify travelers in the TSDB, thereby allowing that individual to use or pass knowledge on to others about how to circumvent the prescreening process, including individuals on the No Fly List. If the known or suspected terrorist successfully evaded the system, numerous barriers to carrying out a potential terrorist attack may not be present, enabling a successful attack.

55. Confirmation that an individual required to undergo enhanced screening is in the TSDB would also allow known or suspected terrorists to more effectively and intelligently plan and carry out a domestic or international attack. Importantly, individuals who are selected for enhanced screening, unlike individuals who are denied boarding, are able to access sterile areas of airports and fly via commercial aviation, which remains a prime target for terrorist groups. Armed with knowledge of TSDB status and limitless opportunities to test screening procedures applicable to Selectees, the individual may rely on social engineering to abbreviate or distract TSA screeners from the screening process. The individual may also rely on insider threats, recruiting insiders to meet onboard the aircraft to obtain the necessary items, such as a soda can converted to an IED, to carry out an attack.

56. The recent international events involving Metrojet Flight 9268 and Daallo Airlines Flight D3-159 highlight the dangers posed at foreign airports, specifically in light of potential insider threats. If the Government is required to broadly confirm the

status of persons required to undergo enhanced screening in the TSDB, terrorists would most certainly use that information in planning attacks on flights bound for the United States. The information could be used to identify the best operatives, to predict the likelihood of detection, and to take countermeasures to attempt to avoid that detection.

57. Required notice of status in the TSDB for persons required to undergo enhanced screening would also allow individuals who were selected for enhanced screening for other reasons unrelated to TSDB status to analyze the specific circumstances in which TSA designates passengers for enhanced screening. For example, an individual selected for enhanced screening based on a TSA risk-based rule that resulted in designation for enhanced screening on multiple consecutive trips could analyze his or her travel patterns in an effort to identify why he or she was designated for enhanced screening. Revealing this information could in turn facilitate the ability of a terrorist unidentified by the United States Government to alter travel plans to avoid being flagged by TSA's risk-based rules. Similarly, revealing status in the TSDB to those required to undergo enhanced screening, even to a limited subset of individuals, could be used to analyze TSA's security measures, including the likelihood of random designation for enhanced screening. The percentage of passengers randomly designated for enhanced screening is informed by current threats and intelligence.

58. TSA continues to effectively counter the grave threat posed by terrorists through enhanced screening. However, giving travelers insight into the circumstances under which an individual may be required to undergo enhanced screening would be detrimental to TSA's countermeasures insofar as terrorists could use the information to predict when TSA would require enhanced screening and to take countermeasures to



avoid such screening. Disclosing TSDB status for passengers required to undergo enhanced screening would most likely lead to TSA randomly designating a substantially higher rate of passengers for enhanced screening and/or deploying additional screening measures, straining screening resources and prolonging the time required for all passengers to complete screening.

59. Finally, the effectiveness of FAMS could be defeated if status in the TSDB of persons required to undergo enhanced screening were disclosed. A public report notes that one of FAMS' objectives is to deploy air marshals on flights that have a known or suspected terrorist on board and that when FAMS assigns air marshals to cover such flights, it refers to these flights as Special Mission Coverage (SMC) assignments. Disclosing status in the TSDB of passengers who are required to undergo enhanced screening would provide valuable knowledge that an armed law enforcement officer may be onboard and that it is simply a matter of identifying that individual and taking measures to obtain his or her firearm or otherwise neutralize that officer to carry out a terrorist attack. FAMS take significant measures to protect their identities in flight and their presence on aircraft to avoid any tactics that could potentially compromise their ability to carry out their mission. Any such disclosure of TSDB status would run counter to FAMS' measures to conceal their identities and FAMS' ability to protect the flight deck and passengers. FAMS in-flight coverage is a highly important, effective, and essential measure to defeating ongoing threats to transportation that would be greatly undermined by disclosing TSDB status to any individual.

60. As explained above, status on the subsets of the TSDB that TSA uses for passenger pre-board screening is SSI and its disclosure is strictly controlled.<sup>35</sup> Moreover, selection for enhanced screening does not signify that an individual is in the TSDB. There are multiple reasons for selecting passengers for enhanced screening other than TSDB status and passengers who are not in the TSDB may be designated for enhanced screening on multiple consecutive flights.

#### TSA's Dissemination of TSDB Information

61. In addition to internally using the TSDB in carrying out its mandate, TSA shares a subset of TSDB information under limited circumstances to further its transportation security mission where it is not otherwise conducting matching of individuals' information against the TSDB. Specifically, TSA provides a subset of TSDB information to regulated U.S. aircraft operators for the purpose of vetting airline employees who may have access to SSI, to regulated U.S. airport operators for the purpose of vetting non-traveling or other individuals who are authorized to have access to the airport,<sup>36</sup> and to regulated U.S. aircraft operators operating charters and other flights under a TSA-authorized security program on aircraft that are not covered by Secure Flight for the purpose of vetting employees and traveling passengers against the No Fly and Selectee subsets of the TSDB. TSA also permits regulated entities who are authorized to receive subsets of the TSDB to share this information with authorized

---

<sup>35</sup> As further explained above, in certain limited circumstances, an individual's No Fly List status is not SSI.

<sup>36</sup> TSA anticipates no longer providing regulated airport operators and aircraft operators with TSDB information and instead conducting this vetting itself in the near future. TSA has already begun this process with respect to airport operators.

representatives with whom they have contracted to perform the vetting function on their behalf.

62. All parties authorized to receive TSDB information by TSA, including authorized representatives, must protect this information as SSI and safeguard this information from unauthorized disclosure in accordance with the provisions of 49 C.F.R. part 1520 and are subject to civil penalty and other enforcement action by TSA if they improperly disclose this information.<sup>37</sup>

### CONCLUSION

63. Disclosing the status in the TSDB of individuals required to undergo enhanced screening would greatly diminish TSA's ability to secure commercial aviation and would provide a significant advantage to determined adversaries. It is essential that the TSDB continue to be confidential for TSA to carry out its crucial mission.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on March 11, 2019

By:

  
Hao-y Tran Froemling  
Executive Director, Vetting  
Office of Intelligence and Analysis  
Transportation Security Administration  
U.S. Department of Homeland Security  
601 South 12th Street  
Arlington, VA 20598

---

<sup>37</sup> In addition, all authorized parties are subject to audits by TSA and must be compliant with DHS and TSA policies regarding sensitive systems and information assurance and complete information security awareness, privacy and SSI training and sign Non-Disclosure Agreements prior to receiving access.

# EXHIBIT A

## **Final Order on Sensitive Security Information**

### **I. Introduction**

Plaintiffs filed suit against various federal agencies in the U.S. District Court for the Eastern District of Virginia. During the course of the litigation, the federal government withheld certain information responsive to discovery requests and deposition questions because they contain Sensitive Security Information (SSI). On March 15, 2018, Plaintiffs filed a motion to compel certain information that is SSI. TSA issues this Final Order addressing the SSI sought by Plaintiffs.

### **II. Authority to Make Final SSI Determinations**

The Administrator of TSA is authorized by 49 U.S.C. § 114(r), formerly 49 U.S.C. § 114(s), and 49 C.F.R. part 1520 to determine whether information pertaining to transportation security constitutes SSI. That authority is delegated from the Administrator to the Chief of the SSI Program pursuant to a Management Directive signed by the Administrator on November 4, 2015. That Management Directive is in effect as of the date of this Final Order.

### **III. Review of Documents and Information**

Pursuant to 49 U.S.C. § 114(r) and 49 C.F.R. part 1520, the SSI Program, under my supervision, has reviewed the documents designated as SSI in Exhibit K to Plaintiffs' first motion to compel and certain information sought in Plaintiffs' first and second motions to compel. These documents were referred to TSA for SSI review after Defendants identified them during discovery, pursuant to 49 C.F.R. § 1520.9(a)(3). In conducting this review, I have determined that 47 documents contain information that falls within the definition of SSI found at 49 C.F.R. § 1520.5.<sup>1</sup> I have also determined that certain information responsive to discovery requests (requests for admission and interrogatories) and deposition questions, which is described in detail below, falls within the definition of SSI found at 49 C.F.R. § 1520.5. I have further determined that the release of this specific information would be detrimental to the security of transportation.

### **IV. Sensitive Security Information Sought by Plaintiffs**

#### ***A. Status of Individuals on the Expanded Selectee List, Selectee List, and No Fly List***

49 C.F.R. § 1520.5(b)(9)(ii) expressly prohibits the disclosure of "[i]nformation and sources of information used by a passenger or property screening program or system, including an automated screening system." This subsection "is intended to cover . . . lists of individuals identified as threats to transportation or national security." Protection of Sensitive Security Information, 69 Fed. Reg. 28066-01, 28071 (May 18, 2004) (interim final rule adding 49 C.F.R. § 1520.5(b)(9)(ii)).

---

<sup>1</sup> The following documents contain SSI: TSCA0001-13, 15, 17-19, TSCB0004-7, 9, 10, 12, 16, 17-37, TSCC0001, 2, 4-6, 10, 11, TSCD0022-24, 26-27, 43, 49, 51, 59, 66, 71, and TSCE0001-3..



The Terrorist Screening Center (“TSC”) maintains the Terrorist Screening Database (“TSDB”), the U.S. government’s consolidated database of identifying information about those known or reasonably suspected of being involved in terrorist activity. TSC exports the No Fly and Selectee lists, subsets of the TSDB, to TSA. TSA also receives and screens passengers against all records in the TSDB that contain a full name and a full date of birth (the “Expanded Selectee list”). Individuals on the No Fly list are prohibited from boarding while individuals on the Selectee and Expanded Selectee lists receive enhanced screening prior to boarding. TSA uses the status of individuals on the No Fly, Selectee, and Expanded Selectee lists when vetting passengers attempting to board commercial aircraft. TSA uses this information to enhance the security of air travel within the United States, to facilitate the secure travel of the public, and to support the federal government’s counterterrorism efforts by assisting in the detection of known or suspected terrorists identified on the No Fly, Selectee, and Expanded Selectee lists who seek to travel by air.

The information I have reviewed includes individuals’ status on the No Fly, Selectee, and Expanded Selectee lists, and information that could be used to ascertain an individual’s current and historical status on those lists. The No Fly, Selectee, and Expanded Selectee lists remain effective tools in the government’s efforts to secure transportation because, among other reasons, their contents are generally not disclosed.<sup>2</sup> Withholding whether or not an individual is on a federal watch list used by TSA for passenger pre-board screening protects the operational counterterrorism and intelligence collection objectives of the federal government and the personal safety of those involved in counterterrorism investigations. If the government revealed the status of individuals as being either on or off the No Fly, Selectee, and Expanded Selectee lists, terrorists and others who seek to circumvent the purpose of those lists would be able to do so, since they would be armed with the knowledge of who would be required to undergo additional screening and who would not. Terrorists could use the information to attempt to evade enhanced security screening at airports and to gain access to the commercial aviation system to perpetrate an attack. Such circumvention of security screening systems would be detrimental to the security of transportation.

Therefore, I determine that disclosure of information that would reveal individuals’ current or historical status on the No Fly, Selectee, or Expanded Selectee lists would be detrimental to the security of transportation. Such information constitutes SSI.<sup>3</sup> In making this determination I have considered the passage of time, intervening changes to the aviation security system, and the evolving security environment.

#### *B. Watchlist Matching Information and Technical IT Details*

<sup>2</sup> In certain limited circumstances, a U.S. citizen or lawful permanent resident who is denied boarding may learn of his or her status on the No Fly List after filing an inquiry with the Department of Homeland Security Traveler Redress Inquiry Program about the denial of boarding. Notwithstanding this exception, which applies in very limited circumstances, TSA has determined previously that any other disclosures of an individual’s status on the No Fly List would be detrimental to the security of transportation in that terrorists could use the information to gain access to the commercial aviation system to perpetrate an attack.

<sup>3</sup> The documents with information falling under this category include, but are not limited to, TSCB0005, 7, TSCC0001, 2, 4-6, 10, 11, and TSCD0051.

49 C.F.R. §§ 1520.5(b)(9)(i) and (b)(9)(ii) expressly prohibit the disclosure of “[a]ny procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons ... that is conducted by the Federal government or any other authorized person”; and “[i]nformation and sources of information used by a passenger or property screening program or system, including an automated screening system.”

Further, 49 C.F.R. §§ 1520.5(b)(4)(i), (b)(13), and (b)(15) expressly prohibit the disclosure of “[a]ny performance specification and any description of a test object or test procedure, for . . . [a]ny device used by the Federal Government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any person. . . .”; “[a]ny information involving the security of operational or administrative data systems operated by the Federal government that have been identified . . . as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems”; and “[i]nformation obtained or developed in the conduct of research related to aviation, maritime, or rail transportation security activities . . . , including research results.”

TSA and TSC rely on applications and technical platforms for both agencies to carry out their functions. Once an identity has been accepted into the No Fly, Selectee, or Expanded Selectee list, that information is exported to TSA through the DHS Watchlist Service.<sup>4</sup> TSA’s Secure Flight system then conducts matching of passenger information to the No Fly, Selectee, and Expanded Selectee lists, which may result in an individual being denied boarding or being required to undergo enhanced security screening.

The information I have reviewed includes the technology and platforms used by TSA and TSC, which culminate in Secure Flight determinations. This includes technical details about Secure Flight, details demonstrating how watchlist matching is conducted, descriptions of software used and connectivity details, and details regarding resolution of a potential match. Secure Flight remains a highly effective tool in the government’s efforts to secure transportation because, among other reasons, this information is not disclosed. This information could be used by adversaries to defeat the Secure Flight system and to circumvent TSA security screening. The technical IT details could be used to obtain unauthorized access to or to otherwise corrupt the systems and the specific matching information, including information about potential matches, could be used to circumvent the matching process. Such actions would be detrimental to the security of transportation.

Therefore, I determine that the disclosure of information about watchlist matching and technical IT details would be detrimental to the security of transportation. Such information constitutes SSI.<sup>5</sup> In making this determination, I have considered the passage of time, intervening changes to the aviation security system, and the evolving security environment.

<sup>4</sup> In July 2010, DHS launched an improved method of transmitting TSDB data to DHS through a service called the DHS Watchlist Service (WLS). WLS maintains a synchronized copy of the TSDB, which contains personally identifiable information and disseminates TSDB records it receives to authorized DHS Components, including TSA.

<sup>5</sup> The documents with information falling under this category include, but are not limited to, TSCC0004-6, 10, and TSCD0049, 59, 66.

*C. TSA Screening Procedures and Security Measures Taken to Counteract Threats*

49 C.F.R. § 1520.5(b)(9)(i) expressly prohibits the disclosure of “[a]ny procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons ... that is conducted by the Federal government or any other authorized person.” 49 C.F.R. § 1520.5(b)(9)(ii) expressly prohibits the disclosure of “[i]nformation and sources of information used by a passenger or property screening program or system, including an automated screening system.” Finally, 49 C.F.R. § 1520.5(b)(8)(i) expressly prohibits the disclosure of “[s]ecurity measures or protocols recommended by the Federal government.”

TSA has the authority to assess threats to transportation and to take appropriate countermeasures to counteract threats, including denying boarding or requiring enhanced security screening. As explained above, individuals on the Selectee and Expanded Selectee lists receive enhanced security screening prior to boarding. TSA also uses intelligence-driven flight by flight risk assessments to identify passengers who require enhanced screening. Under certain circumstances, TSA and other screening agencies may take certain measures upon encountering an individual on the No Fly, Selectee, or Expanded Selectee lists. All of these measures are intended to enhance the security of air travel and to support the government’s counterterrorism efforts.

The information I have reviewed includes procedures and measures that the government may undertake upon encountering individuals on the No Fly, Selectee, and Expanded Selectee lists; the circumstances under which TSA may deny or permit boarding and may require or not require enhanced security screening prior to boarding; the total number of times individuals on the No Fly List have been permitted to fly; the actual screening procedures applied by TSA to individuals on the TSDB; and examples of TSA’s intelligence-driven risk assessments to identify passengers for enhanced security screening, including components of those risk assessments. This information remains effective in the Government’s efforts to secure transportation because, among other reasons, it is not disclosed. If the Government revealed this information, individuals could ascertain whether or not they would be denied boarding or required to undergo enhanced security screening, which in turn could be used by terrorist operatives to plan an attack. Terrorists and others could also take action to evade the procedures and measures, enabling them to circumvent the procedures and measures. Such circumvention would be detrimental to the security of transportation.

Therefore, I determine that disclosing information revealing certain screening procedures and security measures described above would be detrimental to the security of transportation. Such information constitutes SSI.<sup>6</sup> In making this determination I have considered the passage of time, intervening changes to the aviation security system, and the evolving security environment.

*D. Criteria for the TSDB, and the Expanded Selectee, Selectee, and No Fly lists*

49 C.F.R. § 1520.5(b)(9)(ii) expressly prohibits the disclosure of “[i]nformation and sources of information used by a passenger or property screening program or system, including an

---

<sup>6</sup> The documents with information falling under this category include, but are not limited to, TSCA0017-19, TSCB0010, 12, 16, TSCC0010, 11, and TSCD0022, 23, 26, 27, 66, 71.



automated screening system.” Further, 49 C.F.R. § 1520.5(b)(9)(i) expressly prohibits the disclosure of “[a]ny procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons ... that is conducted by the Federal government or any other authorized person.”

TSC reviews nominations to the TSDB to determine whether an individual meets the reasonable suspicion standard for placement on the TSDB, and the heightened criteria for placement on the Selectee and No Fly lists. This review includes consideration of guidance, factors, and examples pertinent to the determination. As further explained above, TSA uses the TSDB to identify individuals who may pose a risk to the transportation system and who should therefore receive enhanced security screening or be denied boarding on an aircraft.

The information I have reviewed includes the current and historical criteria for placement on the Selectee List; guidance, factors, and examples related to whether or not an individual meets the reasonable suspicion standard for placement on the TSDB, and the heightened criteria for placement on the Selectee and No Fly lists; minimum biographic criteria required for TSDB inclusion and export; and nominations information, including prioritization information, related to the timeframe for placing individuals on the TSDB and its subset lists.

All of this information remains effective in the government’s efforts to secure transportation because, among other reasons, it is not disclosed. If the government revealed the Selectee List criteria, information about the application of criteria for the TSDB, the Selectee list, and the No Fly list, terrorists and others who seek to circumvent the purpose of the application of this information would be able to do so by anticipating behavior of concern to the government and changing their behavior in response. Terrorists could also use information related to minimum biographic criteria to evade placement on the TSDB. Further, disclosing changes to the criteria over time would reveal information about the evolving and dynamic threat posed by terrorists. Notwithstanding the public release of the criteria for inclusion on the No Fly List and the reasonable suspicion standard for inclusion on the TSDB, release of the current and historical criteria for the Selectee List would provide adversaries with valuable knowledge of which individuals would present terrorism concerns to the government and of sensitive information related to the threat posed. Unlike individuals on the No Fly List, individuals on the Selectee List and the TSDB are permitted to enter sensitive areas of the nation’s aviation system. Terrorists could also use all of this information to assess the likelihood that other operatives and recruits may have been identified and could use that information to circumvent aviation security measures in planning an attack. Finally, adversaries could use nomination information related to the timeframe for placement on the TSDB to circumvent the purpose of the Expanded Selectee, Selectee, and No Fly Lists, since they would be armed with knowledge of the expedience with which the government could place individuals on those lists. Such circumvention would be detrimental to the security of transportation.

Therefore, I determine that the disclosure of information revealing criteria for placement on the TSDB and its subset lists, as further described above would be detrimental to the security of

transportation. Such information constitutes SSI.<sup>7</sup> In making this determination I have considered the passage of time, intervening changes to the aviation security system, and the evolving security environment.

*E. TSDB and Enhanced Security Screening Statistics*

49 C.F.R. § 1520.5(b)(9)(ii) expressly prohibits the disclosure of “[i]nformation and sources of information used by a passenger or property screening program or system, including an automated screening system.” 49 C.F.R. § 1520.5(b)(7) expressly prohibits the disclosure of “[a]ny information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information.”

The government compiles data related to the number of individuals on the TSDB, and the Expanded Selectee, Selectee, and No Fly lists. This information provides an overview of the number of individuals who are required to undergo enhanced security screening at airports or who are denied boarding. The information I have reviewed includes total numbers of individuals, including U.S. citizens and lawful permanent residents, on the TSDB and its subset lists on a weekly and monthly basis; the current numbers of individuals and U.S. citizens on the Selectee and Expanded Selectee lists; total U.S. citizens on the Selectee List from 2012 to present; the total number of children under age 10 and under age 5 on the TSDB; and the number of times Secure Flight designates individuals for enhanced security screening on a daily and yearly basis.

This information remains effective in the government’s efforts to secure transportation because, among other reasons, it is not disclosed. Revealing the total number of individuals on the TSDB and its subset lists on a weekly and monthly basis, including current numbers and demographic information, would give adversaries valuable operational knowledge about the government’s receipt of intelligence information related to terrorism. For example, if those adversaries had attempted to avoid detection during any given timeframe, those numbers would reveal whether or not they were successful. Similarly, those numbers would reveal the flow of information from other sources related to terrorism. Terrorists could also ascertain the best populations to recruit from if demographic information, such as the number of U.S. citizens and children on the lists, were released.<sup>8</sup> Further, release of the number of individuals who Secure Flight designates for enhanced security screening on a daily and yearly basis would give terrorists and others knowledge about the total percentage of passengers who are designated for enhanced security screening, including by random selection.<sup>9</sup> Such numbers inform adversaries of the likelihood of

<sup>7</sup> The documents with information falling under this category include, but are not limited to, TSCA0001-13, 15, 19, TSCB0004, 6, 9, 12, and 17-37, TSCC0010, TSCD0024, 71, and TSCE0001-3.

<sup>8</sup> The government has made generalized statements about children on the TSDB. Those generalized statements are not SSI. Specific information about the total number of children on the TSDB under five and under ten is SSI in that it would provide adversaries with demographic information that would be useful in determining who to use to perpetrate an attack.

<sup>9</sup> This annualized number constitutes SSI because the number of passengers screened on a yearly basis is publicly available information, and, as a result, an individual with the yearly number of individuals designated for enhanced security screening would know the likelihood of being designated for enhanced security screening at airports. Annualized numbers related to the total number of individuals on the Selectee List are released because such



being designated for enhanced security screening prior to boarding an aircraft. Such knowledge could be used to circumvent TSA's measures to secure commercial aviation, and would be detrimental to the security of transportation.

Therefore, I determine that the disclosure of information about the TSDB and enhanced security screening statistics described above would be detrimental to the security of transportation. Such information constitutes SSI.<sup>10</sup> In making this determination I have considered the passage of time, intervening changes to the aviation security system, and the evolving security environment.

---

numbers do not reveal that likelihood and do not reveal the same trends and patterns as monthly and daily data described above.

<sup>10</sup> The documents with information falling under this category include, but are not limited to, TSCC0001, 2, 11, and TSCD0043.

V. Final Order

This Order is issued under 49 U.S.C. § 114(r) and is final. Pursuant to 49 U.S.C. § 46110, any person disclosing a substantial interest in this Order may, within 60 days of its issuance, apply for review by filing a petition for review in an appropriate U.S. Court of Appeals.

DATED: Arlington, Virginia, April 22, 2018

A handwritten signature in dark ink, appearing to read "Douglas E. Blair", is written over a horizontal line.

DOUGLAS E. BLAIR  
Chief, SSI Program  
Security Services & Assessments Division  
Office of Law Enforcement &  
Federal Air Marshal Service  
Transportation Security Administration  
U.S. Department of Homeland Security